I claim:

1. A method of generating a parameter for a random-number generator, comprising:

(1) generating a value;

(2) using the value to select a prime number;

(3) generating the parameter based on the selected prime number and a second prime number; and

(4) outputting the parameter for use with the random-number generator.

2. The method of claim 1, wherein step 4 comprises:

using the parameter for a linear congruential random-number generator.

3. The method of claim 2, further comprising:

(5) passing an output of the linear congruential random-number generator through a block encryptor.

4. The method of claim 1, further comprising:

(5) using an output of the random number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

5. The method of claim 3, further comprising:

(6) using an output of the random number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

6. The method of claim 1, wherein the second prime number comprises a previously selected prime number.

7. The method of claim 6, wherein step (3) comprises generating the parameter by multiplying the selected prime number by the second prime number.

8. The method of claim 1, wherein step (2) comprises mapping the generated value to the prime number based on a nonlinear distribution function.

9. The method of claim 7, further comprising repeating steps (1) through (3) a plurality of times while the parameter is less than a predetermined value, wherein the parameter generated during each iteration of steps (1) through (3) is a product of a most recently selected one of the selected prime numbers and previously selected prime numbers.

10. A method of generating a parameter for a random-number generator, comprising:

(1) generating a first value;

(2) using the first value to select a first prime number P;

(3) generating a second value;

(4) using the second value to select a number K such that PK is at most equal to a predetermined maximum number;

(5) generating the parameter as a function of PK; and

(6) outputting the parameter for use with the random-number generator .

11. The method of claim 10, further comprising:

(7) generating a third value;

(8) using the third value to select a second prime number;

(9) generating a second parameter by multiplying the selected second prime number by at least one previously selected prime number; and

(10) using the parameter and the second parameter as parameters for the random-number generator.

12. The method of claim 10, wherein act 6 comprises:

using the parameter for a linear congruential random-number generator.

13. The method of claim 11, wherein the random-number generator is a linear-congruential random-number generator.

14. The method of claim 12, further comprising:

(7) passing an output of the linear congruential random-number generator through a block encryptor.

15. The method of claim 13, further comprising:

(11) passing an output of the linear congruential random-number generator through a block encryptor.

16. The method of claim 14, further comprising:

(8) using an output of the linear congruential random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

17. The method of claim 15, further comprising:

(12) using an output of the linear congruential random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

18. The method of claim 11, further comprising repeating acts (7) through (9) a plurality of times while the second parameter is less than a predetermined value, wherein the second parameter generated during each iteration of acts (7) through (9) is a product of a most recently selected one of the selected prime numbers and previously selected prime numbers.

19. An apparatus for generating a parameter for a random-number generator, the apparatus comprising:

means for mapping a random value to a prime number P; and

means for generating the parameter by multiplying the prime number P by at least one previously selected prime number.

20. The apparatus of claim 19, wherein the means for generating produces the parameter for a linear congruential random-number generator.

21. The apparatus of claim 20, further comprising:

a block encryptor, wherein an output of the linear congruential random-number generator is arranged to be passed through the block encryptor.

22. An apparatus for generating a parameter for a random-number generator, the apparatus comprising:

first means for mapping a random value to a prime number P;

second means for mapping a second random value to a number K such that PK is at most equal to a predetermined maximum number; and

means for generating a parameter as a function of PK, wherein the second means for mapping is included within the means for generating.

23. The apparatus of claim 22, wherein the means for generating produces the parameter for a linear congruential random-number generator.

24. The apparatus of claim 22, further comprising:

a block encryptor, wherein an output of the linear congruential random-number generator is arranged to be passed through the block encryptor.

25. A machine-readable medium having information including instructions for a processor recorded thereon, the instructions comprising:

(1) generating a random value;

(2) using the random value to select a prime number;

(3) generating a parameter based on the selected prime number and a second prime number; and

(4) outputting the parameter for use as a parameter for a random number generator.

26. The machine-readable medium of claim 25, wherein step 4 comprises:

using the parameter for a linear congruential random-number generator.

27. The machine-readable medium of claim 26, further having instructions comprising:

(5) passing an output of the linear congruential random-number generator through a block encryptor.

28. The machine-readable medium of claim 27, further having instructions comprising:

(6) using an output of the linear congruential random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

29. The machine-readable medium of claim 25 further having instructions comprising:

(5) using an output of the random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

30. The machine-readable medium of claim 29, further having instructions comprising repeating steps (1) through (3) a plurality of times while the parameter is less than a predetermined value, wherein the parameter generated during each iteration of steps (1) through (3) is a product of a most recently selected one of the selected prime numbers and previously selected prime numbers.

31. A machine-readable medium having instructions recorded thereon for a processor to generate a parameter for a random-number generator, the instructions comprising:

(1) generating a first value;

(2) using the first value to select a first prime number P;

(3) generating a second value;

(4) using the second value to select a number K such that PK is at most equal to a predetermined maximum number; and

(5) generating the parameter as a function of PK .

32. The machine-readable medium of claim 31, further having instructions comprising:

(6) generating a third value;

(7) using the third value to select a second prime number; and

(8) generating a second parameter by multiplying the selected second prime number by at least one previously selected prime number.

33. The machine-readable medium of claim 31, further having instructions comprising:

(6) using the parameter as the parameter of a linear congruential random-number generator.

34. The machine-readable medium of claim 32, further having instructions comprising:

(9) using the parameter and the second parameter as the parameter of a linear congruential random-number generator.

35. The machine-readable medium of claim 33, further having instructions comprising:

(7) passing an output of the linear congruential random-number generator through a block encryptor.

36. The machine-readable medium of claim 34, further having instructions comprising:

(10) passing an output of the linear congruential random-number generator through a block encryptor.

37. The machine-readable medium of claim 35, further having instructions comprising:

(8) using an output of the linear congruential random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

38. The machine-readable medium of claim 36, further having instructions comprising:

(11) using an output of the linear congruential random-number generator to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

39. The machine-readable medium of claim 31, further having instructions comprising:

using the parameter as the parameter for the random-number generator, wherein

an output of the random-number generator is used to establish a pseudo-randomly selected network address that is used to transmit a digital computer message.

40. The machine-readable medium of claim 32, further having instructions comprising repeating acts (6) through (8) a plurality of times while the second parameter is less than a predetermined value, wherein the second parameter generated during each iteration of acts (6) through (8) is a product of a most recently selected one of the selected prime numbers and previously selected prime numbers.

41. The method of claim 1, wherein step 2 comprises:

searching through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the parameter and a corresponding one of the weights.

42. The method of claim 10, wherein step 2 comprises:

searching through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the first parameter and a corresponding one of the weights.

43. The apparatus of claim 19, wherein the prime number mapper is arranged to search through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the random value and a corresponding one of the weights.

44. The apparatus of claim 22, wherein the prime number mapper is arranged to search through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the random value and a corresponding one of the weights.

45. The machine-readable medium of claim 25, wherein step 2 comprises:

searching through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the random value and a corresponding one of the weights.

46. The machine-readable medium of claim 31, wherein step 2 comprises:

searching through an ordered table of entries, each of the entries including a prime number and a weight, a respective prime number from one of the entries being selected based on the first value and a corresponding one of the weights.

47. The method of claim 1, wherein step (1) comprises generating a random value.

48. The method of claim 10, wherein step (1) comprises generating a random value.

49. The method of claim 10, wherein step (3) comprises generating a random value.

50. The method of claim 11, wherein step (7) comprises generating a random value.

51. The machine-readable medium of claim 25, wherein the second prime number comprises a previously selected prime number.

52. The machine-readable medium of claim 51, wherein step (3) comprises generating the parameter by multiplying the selected prime number by the second prime number.

53. The method of claim 1, further comprising repeating steps (1) – (4) for a plurality of random number generators.